10/048057
JC13 Rec'd PCT/PTO 25 JAN 2002

T2147-907642-US 3897/HD(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant:	Michel HABERT
International Application No.:	PCT/FR01/01564
International Filing Date:	22 May 2001
U.S. Serial No.:	To be assigned
U.S. Filing Date:	January 25, 2002
For:	**METHOD AND SYSTEM ARCHITECTURE FOR SECURE COMMUNICATION BETWEEN TWO ENTITIES CONNECTED TO AN INTERNET NETWORK COMPRISING A WIRELESS TRANSMISSION SEGMENT**

McLean, Virginia
January 25, 2002

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The following amendments and remarks are submitted prior to examination of the above-identified application on the merits.

IN THE SPECIFICATION:

Before the paragraph numbered **[0001]**, insert the following heading:

--BACKGROUND OF THE INVENTION

1. Field of the Invention.--;

Before the paragraph numbered **[0006]**, insert the following heading:

10048057 .012502

--2. Description of the Related Art.--;

Before the paragraph numbered **[0038]**, insert the following heading:

--SUMMARY OF THE INVENTION--;

Before the paragraph numbered **[0047]**, insert the following heading:

--BRIEF DESCRIPTION OF THE DRAWINGS--;

Before the paragraph numbered **[0048]**, insert the following heading:

--DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

10048057.012502

Page 17, after paragraph **[0097]**, insert the following new paragraph:

--**[0098]** While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

Page 18, after the heading "CLAIMS" and before the first claim, insert the following:

--We claim:--

10048057.012502

IN THE CLAIMS

Please substitute amended claims 1-18 as presented below for the same-numbered claims that were pending prior to the filing of this paper. A marked-up version of the amended claims is attached.

1. (Amended) A method for secure communication between first and second entities interconnected via an internet network, said entities being associated with respective first and second processing systems connected to said internet network, said first system operating in client mode and said second system operating in server mode, said method comprising:

assigning respective permanent internet addresses to said first and second entities,

making at least one application, located in a server of said second system, accessible to said first entity, and

encrypting data exchanged between said first and second entities in conformity with a desired security protocol, wherein said first and second systems include a communication protocol stack having at least one layer which allows for said encrypting step to be performed.

2. (Amended) A method according to claim 1, wherein said permanent IP addresses assigned to said first and second entities conform to an IPV6 Internet address protocol.

3. (Amended) A method according to claim 2, wherein communications through said internet network take place in conformity with an IPV4 Internet address protocol, and wherein said method further comprises:

executing, in at least one of said first and second systems, an address conversion step which includes converting said IPV4 internet address protocol to said IPV6 internet address protocol.

10045057.012502

4. (Amended) A method according to claim 1, wherein said encrypting step is performed in conformity with an IPSec protocol in tunnel mode, in order to obtain secure data exchanges between said first and second entities, and wherein said IPSec protocol is used with an EPS mechanism for authenticating information sources.

5. (Amended) A method according to claim 4, wherein said first entity is a user of said first system, wherein said method further includes a step for authenticating said user, and wherein said permanent IP address assigned to said first entity is used to identify said user.

6. (Amended) A method according to clam 5, wherein communications through said network take place in data packet mode, and wherein said permanent IP address identifying said user is present in encrypted form in conformity with said IPSec protocol, in each of said data packets.

7. (Amended) A method according to claim 1, wherein said first system is connected to a wireless transmission segment,

wherein communications between said first system and said second system take place in conformity with a WAP protocol, and

wherein said second system includes a WAP server and a unified interface between said WAP server and at least one application, said at least one application being located in said second system and being accessible by said first entity, and

wherein said WAP server is integrated into said second system as a web server.

8. (Amended) A method according to claim 7, wherein said second system includes an additional module for performing two-way interface adaptation of structures, which makes it possible to support application interfaces used by web servers.

9. (Amended) A method according to claim 7, wherein said first system includes a WAP browser.

10. (Amended) A method according to claim 1, wherein said first system includes a mobile system,

wherein said method further includes assigning to said first system a temporary address, and initiating a dialog between said first system and a home agent connected to said internet network to correlate said permanent address

10048057.012502

assigned to said first entity with said temporary address, in conformity with said IPV6 protocol.

11. (Amended) A system architecture for secure communication between first and second entities interconnected via an internet network, said entities respectively being associated with first and second data processing systems within a set of distributed systems connected to said internet network, said first system operating in client mode and said second system operating in server mode, said first and second entities being associated with permanent internet addresses, comprising:

a server included in said second system, said server comprising at least one application accessible to said first entity;

first and second communication protocol stacks respectively included in said first and second systems, each of said first and second communication protocol stacks comprising at least one address layer using a respective one of said permanent IP addresses and a logical layer for encrypting, in end-to-end mode in conformity with a given security protocol, data exchanged between said first and second entities.

10048057 .012502

12. (Amended) An architecture according to claim 11, wherein said address layer conforms to an IPV6 protocol.

13. (Amended) An architecture according to claim 12, wherein said internet network conveys data packets in conformity with an IPV4 protocol,

wherein each of said first and second protocol stacks includes a first address layer in the IPV6 protocol and a second address layer in the IPV4 protocol from which IPV6-compatible addresses are derived, in order to obtain exchanges in tunnel mode, and

wherein said logical layer in each of said first and second protocol stacks encrypts data packets exchanged between said first and second entities.

14. (Amended) An architecture according to claim 11, wherein said logical layer in each of said first and second protocol stacks conforms to an IPSec protocol in tunnel mode, in order to obtain secure data exchanges between said interconnected first and second_entities, and wherein said IPSec protocol is used with an EPS mechanism for identifying information sources.

10048057.012502

15. (Amended) A method according to claim 11, wherein said first system is connected to a wireless transmission segment wherein communications between said first system and said second system take place in conformity with a WAP protocol, wherein said second system includes at least a first module constituting a WAP server and a second module forming a unified interface between said WAP server and said at least one application, and wherein said WAP server is integrated into said second system as a web server.

16. (Amended) An architecture according to claim 15, wherein said second system includes at least one additional module for two-way conversion of data packets of structures in conformity with web or WAP protocols.

17. (Amended) An architecture according to claim 15, wherein said first system is a mobile telephone terminal operating in a GSM standard, said mobile telephone terminal including a WAP type browser constituting a client and a display screen for displaying pages in WML-type language.

18. (Amended) An architecture according to claim 15, wherein said first system is a mobile telephone terminal operating in a GPRS standard, said mobile telephone terminal including an Internet browser constituting a client and a display screen for displaying pages in WML-type language.

10048057.012502

IN THE ABSTRACT

Please replace the Abstract as originally filed with the following new abstract:

-- ABSTRACT

A method for providing secure communication between first and second systems connected to the internet includes assigning respective permanent internet addresses to first and second entities associated with the systems, making at least one application located in a server of said second system accessible to the first entity, and encrypting data exchanged between the first and second entities in conformity with a desired security protocol. The first and second systems each include a communication protocol stack having at least one layer which allows for the encrypting step to be performed. Through this method, a user in the first system can directly address an application hosted by the second system without using or even knowing the name of the host system. The entity in the first system may be a wireless unit operating, for example, in GSM and the entity in the second system may be a server in an intranet. To enable conversion to take place between the wireless application and internet standards, the server in the second system is preferably equipped with WAP and WEB servers and associated conversion units. --

10048057.012502

REMARKS

Claims 1-18 are pending. These claims have been amended to place them in a form which comports with established U.S. claim practice. Also, the specification has been amended to include section headers, and a new abstract has been provided.

It is respectfully submitted that the application is in condition for allowance. Favorable consideration and prompt allowance of the application is respectfully requested.

Should the Examiner believe that further amendments are necessary to place the application in condition for allowance, or if the Examiner believes that a personal interview would be advantageous in order to more expeditiously resolve any remaining issues, the Examiner is invited to contact Applicants' undersigned attorney at the telephone number listed below.

To the extent necessary, Applicants petition for an extension of time under 37 CFR § 1.136. Please charge any shortage in fees due in connection with this application, including extension of time fees, to Deposit Account No. 50-1165

10048057.012502

(Attorney Docket No. T2147-907642) and credit any excess fees to the same Deposit Account.

Respectfully submitted,

Samuel W. Ntiros
Registration No. 39,318

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone No: (703) 610-8641
Facsimile No: (703) 610-8686

10048057.012502

Marked-Up Version of the Amended Claims

1. (Amended) A method [Method] for secure communication between first and second entities interconnected via an internet network, said entities being associated with respective first and second [computer data] processing systems [within a set of distributed systems] connected to said internet network, [characterized in that said first and second entities are constituted by a piece of software (36*a*-36*b*, 37*a*-37*b*) hosted in one of said systems (3, 3') connected to said internet network (*RI*, *R*) and/or a user (U_1) of said connected systems (4, 20), in that] said first system [(4, 20) operates in the so-called] operating in client mode and said second system [(3, 3') operates in the so-called] operating in server mode, [in that it includes a step for] said method comprising:

assigning[, in said set of systems, a] respective permanent [Internet] internet addresses [address of the so-called IP type to each of] said [interconnected] first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*), in that installed in]

making at least one application, located in a server of said second system, [forming the server (3, 3') is at least one piece of software forming a server (30, 31) and offering the services of at least one application (36a-36b, 37*a*-37d)] accessible to said first entity[(U_1)], and

encrypting data exchanged between said first and second entities in conformity with a desired security protocol, wherein [in that installed in] said first [(4, 20)] and second [(3, 3')] systems include [is] a communication protocol stack [that includes] having at least one layer [(45, 391)] which allows for said encrypting step to be performed [the execution of a step for encrypting, in end-to-

10047057.012502

end mode in conformity with a given security protocol, data exchanged between said interconnected entities (U_1, 36*a*-36*b*, 37*a*-37*d*)].

2. (Amended) A method [Method] according to claim 1, [characterized in that] wherein said permanent IP addresses assigned to said [interconnected] first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*)] conform to [the] an IPV6 Internet address protocol.

3. (Amended) A method [Method] according to claim 2, [characterized in that since said] wherein communications through said internet network [(*RI*, *R*)] take place in conformity with [the] an IPV4 Internet address protocol, [it includes the installation in said first (4, 20) and second (3, 3') systems of a protocol layer (46, 392) that makes it possible to derive IPV4 addresses that are compatible with said IPV6 protocol, by] and wherein said method further comprises:

executing, in at least one of said first and second systems, an address conversion step which includes converting said IPV4 internet address protocol to said IPV6 internet address protocol [that conforms to the so-called "6-to-4" protocol].

4. (Amended) A method [Method] according to claim 1, [characterized in that said encryption] wherein said encrypting step is performed in conformity with [the so-called] an IPSec protocol[, used with the so-called EPS mechanism for authenticating information sources,] in [the so-called] tunnel mode, in order to obtain secure data exchanges between said [interconnected] first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*)], and wherein said IPSec protocol is used with

10048057.012502

an EPS mechanism for authenticating information sources.

5. (Amended) A method [Method] according to claim 4, [characterized in that,] wherein said first entity [being] is a user [(U_1)] of said first system [(4, 20), it], wherein said method further includes a step for authenticating said user [(U_1)], and wherein [and in that] said permanent IP address assigned to said first entity is used [as data for identifying this] to identify said user [(U_1)].

6. (Amended) A method [Method] according to clam 5, [characterized in that since said] wherein communications through said network take place in data packet mode, and wherein said permanent IP address [data for] identifying [a] said user [(*U*1)] is present in encrypted form in conformity with said IPSec protocol, in each of said data packets.

10048057.012502

7. (Amended) A method [Method] according to claim 1, [characterized in that] wherein said first system [(4, 20)] is connected to a wireless transmission segment [(*RTT*)], [in that the]

wherein communications between [this] said first system [constituting a client system (4, 20)] and said second system [constituting a server system (3, 3')] take place in conformity with [the so-called] a WAP protocol, and [in that it includes the installation in]

wherein said second system [(3, 3') of at least one piece of software constituting] includes a WAP server [(30)] and a [second piece of software (32) forming a] unified interface between said WAP server [(30)] and at least one application [(36*a*-36*b*, 37*a*-37*d*)], said at least one application being located in said second system and being accessible by [offering its services to] said first entity [(U_1), so that] and

wherein said WAP server [(30)] is integrated into said [server] second system [(3, 3')] as a web server.

8. (Amended) A method [Method] according to claim 7, [characterized in that it includes the installation in] wherein said second system [(3, 3') of] includes an additional module [(35)] for performing two-way interface adaptation of structures, which makes it possible to support application interfaces [(33)] used by web servers.

10048057.012502

9. (Amended) A method [Method] according to claim 7, [characterized in that it includes the installation in] wherein said first system [(4, 20) of a piece of software constituting a client and in that said piece of software is] includes a WAP browser.

10. (Amended) A method [Method] according to claim 1, [characterized in that,] wherein said first system [being] includes a mobile system [(25), it],

wherein said method further includes [the assignment] assigning to said first system [(25) of] a temporary address, and [in that it includes a step for] initiating a dialog between said first system [(25)] and [an element called] a ["]home agent[" (23)] connected to said internet network [(*it*), which makes it possible] to correlate[, at all times,] said permanent address assigned to said first entity [(U'_3)] with said temporary address, in conformity with said [the so-called "mobile] IPV6 protocol["].

11. (Amended) A system [System] architecture for secure communication between first and second entities interconnected via an internet network, said entities respectively being associated with first and second [computer] data processing systems within a set of distributed systems connected to said internet network, [characterized in that] said first system [(4, 20) is a system] operating in [the so-called] client mode and said second system ([3, 3') is a system] operating in [the so-called] server mode, [in that said first and second entities are pieces of software (36*a*-36*b*, 37*a*-37*d*) hosted in said first (4, 20) and second (3, 3') systems and/or a user (U_1) of said connected systems, in that] said first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*) are] being associated with permanent [Internet] internet addresses [of the so-called IP type, in that said second system (3, 3') forming the], comprising:

a server included in said second system, said server comprising [comprises at least one piece of software (31) forming a server (30, 31) and offering the services of] at least one application [(36*a*-36*b*, 37*a*-37*d*)] accessible to said first entity [(U_1), and in that said first (4, 20) and second (3, 3') systems include a]

first and second communication protocol [stack] stacks respectively included in said first and second systems, each of said first and second communication protocol stacks comprising at least one address layer [(44, 390)] using a respective one of said permanent IP [address] addresses and a logical layer [(45, 391) for the execution of a step] for encrypting, in end-to-end mode in conformity with a given security protocol, data exchanged between said first and second [interconnected] entities [(U_1, 36*a*-36*b*, 37*a*-37*d*)].

10045057.012502

12. (Amended) An architecture [Architecture] according to claim 11, [characterized in that] wherein said address layer [(44, 390)] conforms to [the] an IPV6 protocol.

13. (Amended) An architecture [Architecture] according to claim 12, [characterized in that since] wherein said internet network [(*R*)] conveys data packets in conformity with an [the] IPV4 protocol,

wherein each of said first and second protocol stacks [of said first (4, 20) and second (3, 3') systems each include] includes a first address layer [(44, 390) using said IP address] in the IPV6 protocol[,]and a second address layer [(46, 392)] in the IPV4 protocol from which IPV6-compatible addresses are derived, in order to obtain exchanges in [the so-called] tunnel mode[;], and

wherein said logical layer [layers (45, 391) executing an encryption step (45,37) in favor of said] in each of said first and second protocol stacks encrypts data packets exchanged between said [interconnected] first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*)].

14. (Amended) An architecture [Architecture] according to claim 11, [characterized in that] wherein said logical layer [layers (45, 391) for executing an encryption step conforms] in each of said first and second protocol stacks conforms to [the so-called] an IPSec protocol[, used with the so-called EPS mechanism for identifying information sources,] in [the so-called] tunnel mode, in order to obtain secure data exchanges between said interconnected first and second entities [(U_1, 36*a*-36*b*, 37*a*-37*d*)], and wherein said IPSec protocol is used with an EPS mechanism for identifying information sources.

10045057.012502

15. (Amended) A method [Method] according to claim 11, [characterized in that] wherein said first system [(4, 20)] is connected to a wireless transmission segment [(*RTT*), in that the] wherein communications between [this] said first system [(4, 20) constituting a client system] and said second system [(3, 3') constituting a server system] take place in conformity with [the so-called] a WAP protocol, [and in that] wherein said second system [(3, 3')] includes at least a first module constituting a WAP server [(30)] and a second module [(32)] forming a unified interface between said WAP server [(30)] and said at least one application [(36*a*-36*b*, 37*a*-37*d*) offering its services to said first entity (U_1), so that], and wherein said WAP server [(30)] is integrated into said [server] second system [(3, 3')] as a web server.

10048057 .012502

16. (Amended) An architecture [Architecture] according to claim 15, [characterized in that] wherein said second system [(3, 3')] includes at least one additional module [(38*a*-38*b*)] for [the] two-way conversion of data packets of structures in conformity with [said] web or WAP protocols.

17. (Amended) An architecture [Architecture] according to claim 15, [characterized in that] wherein said first system is a mobile telephone terminal [(20, 4)] operating in a [the so-called] GSM standard, [in that it includes] said mobile telephone terminal including a WAP type browser constituting a client[,] and [in that it includes] a display screen for displaying pages in [a] WML-type language [of the so-called WML type].

18. (Amended) An architecture [Architecture] according to claim 15,

[characterized in that] wherein said first system is a mobile telephone terminal operating in [the so-called] a GPRS standard, [in that it includes] said mobile telephone terminal including an Internet browser constituting a client[,] and [in that it includes] a display screen for displaying pages in [a] WML-type language [of the so-called WML type].

10045057 .012502

10048051 .012502

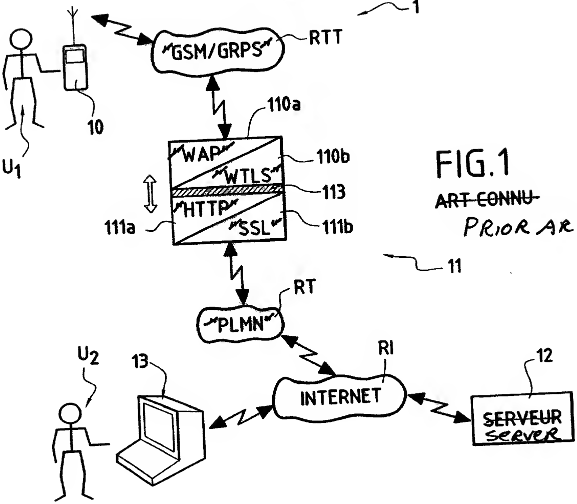

1
RTT
"GSM/GRPS"
10
U1
110a
"WAP"
"WTLS"
110b
113
"HTTP"
"SSL"
111a
111b
11
RT
"PLMN"
U2
13
RI
12
INTERNET
~~SERVEUR~~
SERVER

FIG.1

~~ART CONNU~~

PRIOR ART

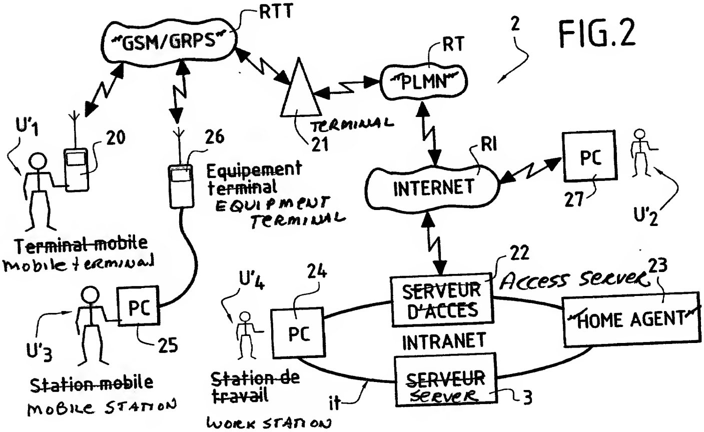

RTT
"GSM/GRPS"
2
RT
"PLMN"
U'1
20
26
TERMINAL
21
Equipement terminal
EQUIPMENT TERMINAL
RI
PC
INTERNET
27
U'2
~~Terminal mobile~~
Mobile terminal
22
U'4
24
Access server
23
~~SERVEUR D'ACCES~~
"HOME AGENT"
PC
U'3
25
PC
INTRANET
~~Station mobile~~
MOBILE STATION
~~Station de travail~~
WORK STATION
it
~~SERVEUR~~
SERVER
3

FIG.2

10048057 .012502

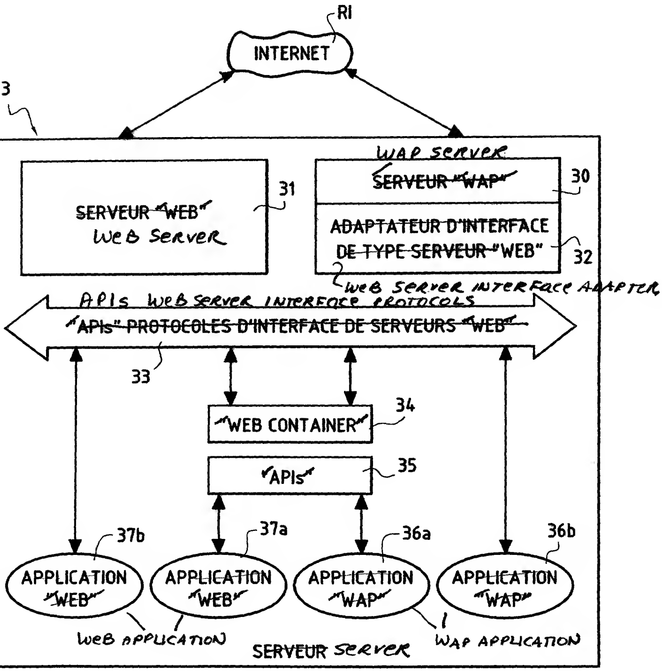

RI
INTERNET
3
WAP SERVER
~~SERVEUR "WAP"~~
30
31
~~SERVEUR "WEB"~~
WEB SERVER
~~ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"~~
32
WEB SERVER INTERFACE ADAPTER
APIs WEB SERVER INTERFACE PROTOCOLS
~~"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"~~
33
~~"~~WEB CONTAINER~~"~~
34
~~"~~APIs~~"~~
35
37b
37a
36a
36b
APPLICATION ~~"~~WEB~~"~~
APPLICATION ~~"~~WEB~~"~~
APPLICATION ~~"~~WAP~~"~~
APPLICATION ~~"~~WAP~~"~~
WEB APPLICATION
WAP APPLICATION
~~SERVEUR~~ SERVER

FIG.3

10048057 . 012502

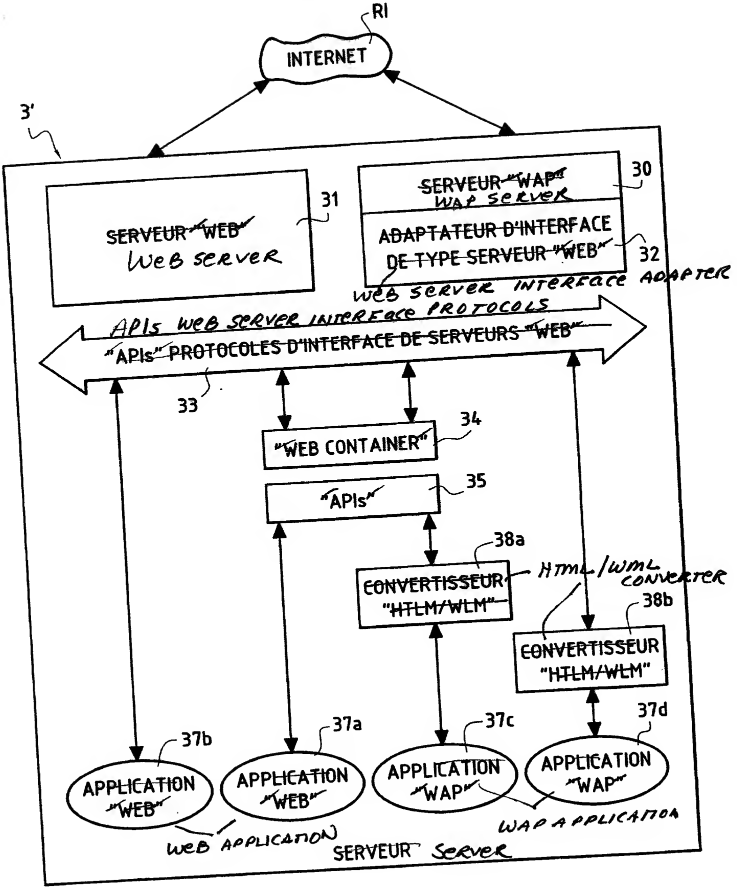
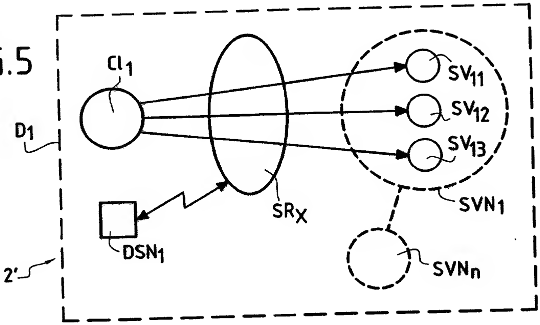

RI
INTERNET
3'
~~SERVEUR "WEB"~~
Web server
31
~~SERVEUR "WAP"~~
WAP server
30
~~ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"~~
Web server interface adapter
32
APIs web server interface protocols
~~"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"~~
33
"WEB CONTAINER"
34
"APIs"
35
38a
~~CONVERTISSEUR "HTLM/WLM"~~
HTML/WML converter
38b
~~CONVERTISSEUR "HTLM/WLM"~~
37b
~~APPLICATION "WEB"~~
37a
~~APPLICATION "WEB"~~
37c
~~APPLICATION "WAP"~~
37d
~~APPLICATION "WAP"~~
Web application
WAP application
~~SERVEUR~~ Server

FIG.4

10048057.012502

FIG.5


Cl1
D1
SV11
SV12
SV13
SRX
SVN1
DSN1
SVNn
2'

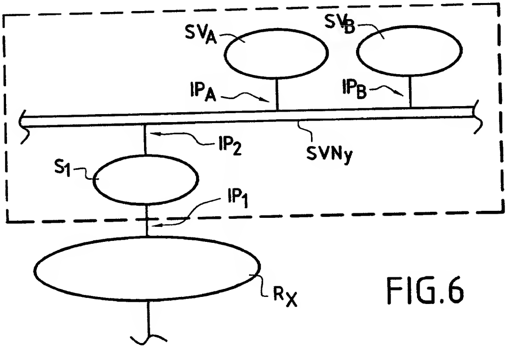
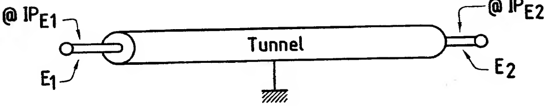

SVA
SVB
IPA
IPB
IP2
SVNy
S1
IP1
RX

FIG.6

FIG.8


@ IPE1
@ IPE2
Tunnel
E1
E2

10048057 .012502

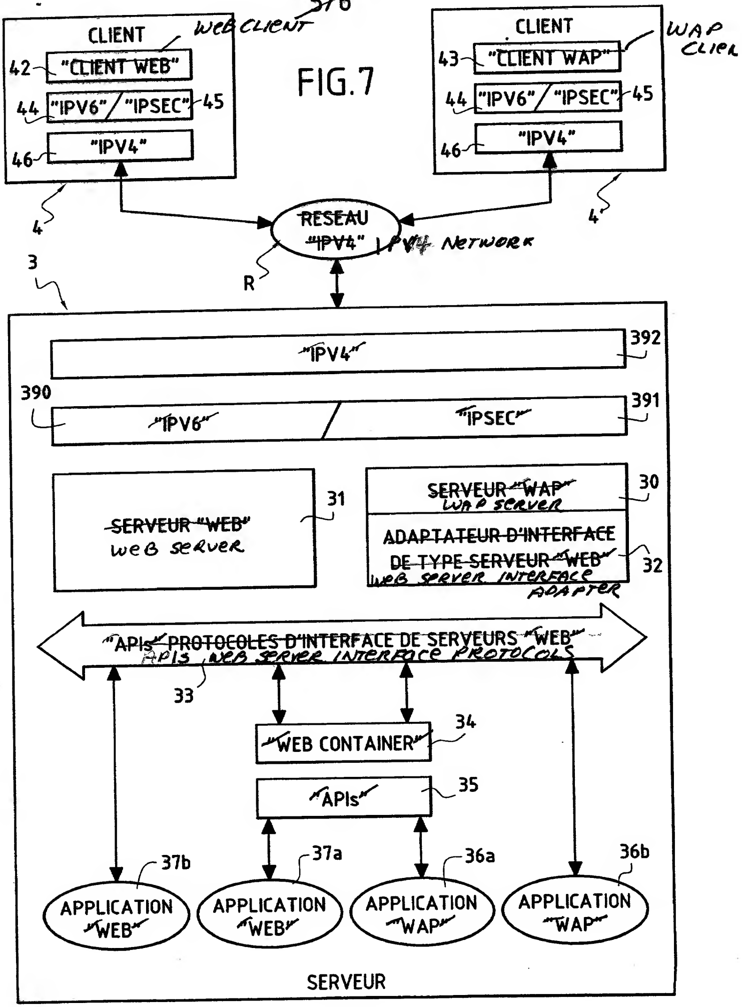
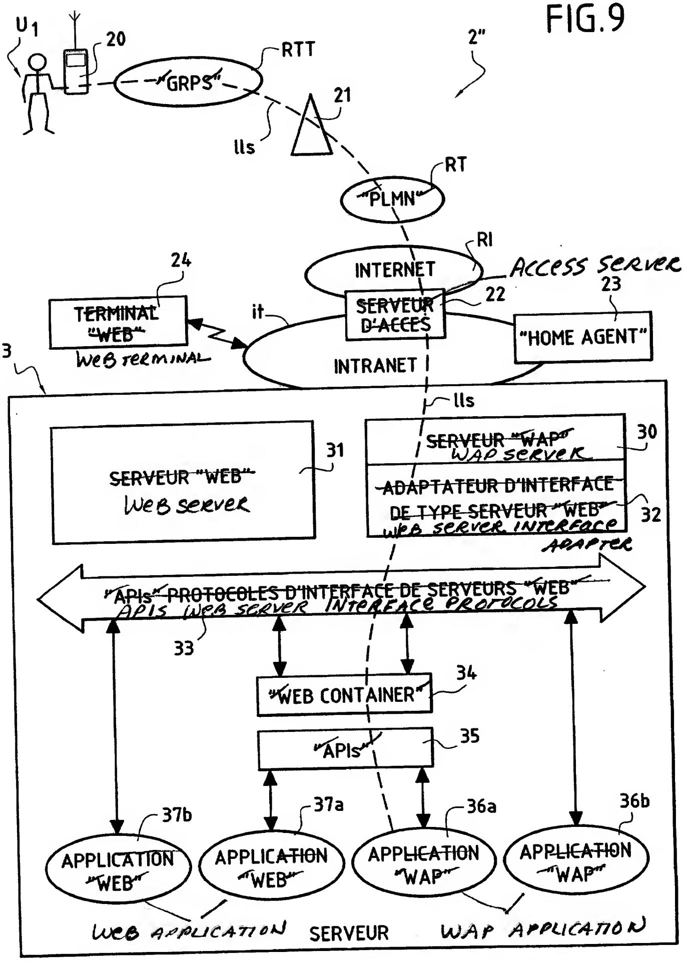

CLIENT
WEB CLIENT
42
"~~CLIENT WEB~~"
44
"IPV6"/"IPSEC"
45
46
"IPV4"
4
CLIENT
WAP CLIEN
43
"~~CLIENT WAP~~"
44
"IPV6"/"IPSEC"
45
46
"IPV4"
4'
~~RESEAU "IPV4"~~
IPV4 NETWORK
R
3
"IPV4"
392
390
"IPV6"
"IPSEC"
391
~~SERVEUR "WEB"~~
WEB SERVER
31
~~SERVEUR "WAP"~~
WAP SERVER
30
~~ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"~~
WEB SERVER INTERFACE ADAPTER
32
"APIs" ~~PROTOCOLES D'INTERFACE DE SERVEURS "WEB"~~
APIs WEB SERVER INTERFACE PROTOCOLS
33
"WEB CONTAINER"
34
"APIs"
35
37b
37a
36a
36b
APPLICATION "WEB"
APPLICATION "WEB"
APPLICATION "WAP"
APPLICATION "WAP"
SERVEUR

FIG.7

FIG.9


U1
20
RTT
~~"GRPS"~~
2"
21
lls
RT
~~"PLMN"~~
RI
INTERNET
Access server
23
22
~~SERVEUR D'ACCES~~
24
~~TERMINAL "WEB"~~
Web terminal
it
"HOME AGENT"
INTRANET
3
lls
~~SERVEUR "WAP"~~
WAP server
30
31
~~SERVEUR "WEB"~~
Web server
~~ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"~~
web server interface adapter
32
~~"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"~~
APIs web server interface protocols
33
34
~~"~~WEB CONTAINER~~"~~
35
~~"~~APIs~~"~~
37b
37a
36a
36b
~~APPLICATION "WEB"~~
~~APPLICATION "WEB"~~
~~APPLICATION "WAP"~~
~~APPLICATION "WAP"~~
Web application
SERVEUR
WAP application